THE RIGHT STUFF 'v' THE RIGHT (SAFE) THING

Dr Andy Quinn MSc PhD MRAeS CEng (1), Dr Ivan Sikora MSc PhD MRAeS FHEA (2)

(1) Saturn Safety Management Systems Ltd, Bath, BA2 9BR, UK

(2) City University, London, EC1V 0HB, UK

ABSTRACT

This is not the 1950's where test pilots needed the 'right stuff' and certainly not the beginning of aviation where the Wright brother's early designs needed pilots with more than the right stuff. In those formative years of aviation and jet development, designers and pilots did not have the same design understanding and knowledge that we have today. In addition, they did not have the same understanding and knowledge of Systems Safety engineering and Human Factors expertise that we have today. Manned suborbital flights of today should be undertaken in vehicles that have been designed effectively with appropriately derived safety requirements including fault-tolerance, safe life and design-for-minimum risk approaches – and all to an acceptable level of safety. Therefore, although initial suborbital pilots will originate from flight test schools and still possess similar traits to their earlier test pilot brethren, they should be protected by the *right (safe) thing* by design and analysis rather than rely on the *right stuff* due to ineffective design and operating procedures. The paper presents a review of the SpaceShip2 accident as a case study to highlight the right (safe) things that should be considered in the design, analysis and operations for suborbital operators. The authors of this paper contend that suborbital piloted vehicles should be designed with the knowledge and understanding and lessons learned from those early X-plane flights, lessons learned from general space safety, lessons learned from pilot Human Factors/ Crew Resource Management training and by understanding that safety management and safety engineering are essential disciplines that should be integrated with the design team from the concept phase.

1. INTRODUCTION

During the early days of airliners, military fast jet and rocket development, aircraft were plagued by technical issues that resulted in incidents and accidents. In the case of US fast jet and rocket development on the X-15 project, this meant relying on pilots with the 'right stuff'. Consequently, throughout the project, this meant reactive fixes to the reliability and design issues i.e. 'fly, fix, fly'. As technology and complexity improved over time, causal factors identified in incidents and accidents are more plagued by people and organisations. To counter this, technical designers are now being supported by other engineering disciplines including human factors and systems safety engineering:

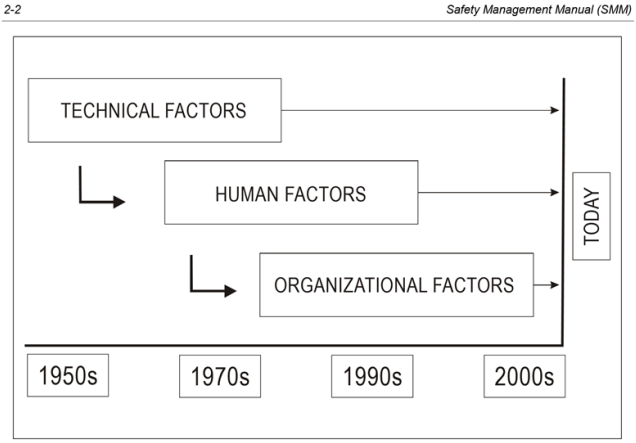

Figure 1: Evolution of Safety Thinking [1]

2. REVIEW OF ACCIDENT CREW CASUAL FACTORS

Based on National Transportation Safety Board (NTSB) sources of significant crew causal factors in 93 major hull losses from 1977-1984, Lautman and Gallimore [2] found that pilot deviation and inadequate cross-check were the main causal factors:

- **33% - Pilot deviated from SOP's**
- **26% - Inadequate cross check by second crew member**
- 9% - Crew's not trained for correct response in emergency situations
- 6% - Pilot did not recognise need for go-around
- 4% - Pilot Incapacitation
- 4% - Inadequate piloting skills

- 3% - Improper procedure during go-around
- 3% - Crew errors during training flight
- 3% - Pilot not conditioned to respond promptly to Ground Proximity Warning
- 3% - Inexperienced on ac type

The findings are backed up in a more recent Boeing study as presented by NTSB senior expert, Sumwalt [3]:

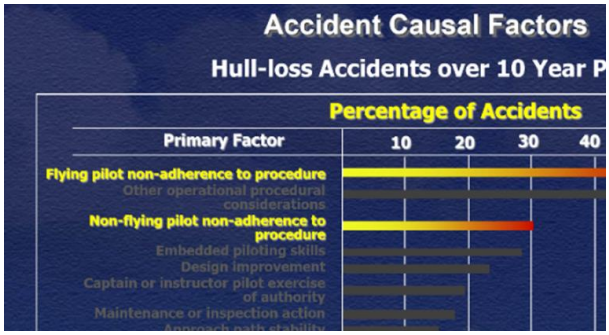

Figure 2: Accident Causal Factors – Extract from Sumwalt Presentation

3. REVIEW OF SPACESHIP 2 ACCIDENT

During Powered Flight number four (PF04) SpaceShip2 (SS2) suffered an in-flight break-up shortly after rocket motor ignition. This was due to uncommanded deployment of the feathering device at Mach 0.8 and under the aerodynamic loads tore the vehicle apart. The NTSB conclusions [4] had no doubt that the initiating (causal) factor was the co-pilot, as non-handling pilot, incorrectly unlocking the feathering device by operating the arming lever early (at Mach 0.8 instead of Mach 1.4). The NTSB concludes that the co-pilot was experiencing **high workload** as a result of recalling tasks from memory while performing under **time pressure** and with **vibration and loads** that he had not recently experienced, which increased the opportunity for errors. The NTSB notes that Scaled did not recognize and mitigate the possibility that a test pilot could unlock the feather early.

The accident co-pilot was the co-pilot of SS2 on **seven glide flights** occurring between October 10, 2010, and August 28, 2014. He had been the co-pilot of SS2 for PF01 (**one powered flight**) on April 2013.

The co-pilot, age 39, held an airline transport pilot (ATP) certificate with a rating for airplane multi-engine land and commercial pilot privileges for airplane single-engine land and sea and glider. The co-pilot held a second-class medical certificate, dated May 22, 2014, with the limitation that he must wear corrective lenses. The cockpit image recording showed that the co-pilot was wearing glasses during the accident flight.
The NTSB concluded that the pilot and co-pilot were properly certificated and qualified.

3.1. ANALYSIS VERSUS NTSB KNOWN (AVIATION) CREW CASUAL FACTORS

The NTSB research into crew casual factors in aircraft accidents (para. 2 above) found that the top two factors were (i) *pilot deviated from SOPs* and (ii) *Inadequate cross check by second crew member*. These causal factors appear to be the same for the SS2 accident.

The Scaled Composites' SS2 co-pilot came from the aviation domain, and he would have been aware of the need for effective Crew Resource Management (CRM). CRM is defined [5] as;

'a set of training procedures for use in environments ***where human error can have devastating effects.*** *Used primarily for improving air safety, CRM focuses on interpersonal communication, leadership, and decision making in the cockpit*'

As the definition implies, CRM is not related to the technical knowledge and flying skills of pilots but rather with the interpersonal skills and cognitive skills i.e. the ability to communicate, maintaining situational awareness and for solving problems and making effective decisions.

Designs should not rely on pilots having the 'right stuff' all of the time. Indeed, the Federal Aviation Administration Office of Commercial Space Transportation (FAA-AST) §460.15 [6] detail the following human factors requirements:
An operator must take the precautions necessary to account for human factors that can affect a crew's ability to perform safety-

critical roles, including in the following safety critical areas—
(a) Design and layout of displays and controls;
(b) Mission planning, which includes analysing tasks and allocating functions between humans and equipment;
(c) Restraint or stowage of all individuals and objects in a vehicle; and
(d) Vehicle operation, so that the vehicle will be operated in a manner that flight crew can withstand any physical stress factors, such as acceleration, vibration, and noise.

Note item (d) above in relation to the NTSB findings detailed in bold further above in para. 3.

Additionally, in terms of being able to withstand any physical stress factors, FAA-AST launch licensing requirements detail the crew requirements, including pilot experience and medical requirements [6].

However, the IAASS [7] and Aerospace Medical Association (AsMA) [8] recommend that suborbital spaceplane pilots have a first-class medical certificate (not a second-class, as recommended by the FAA-AST) and be selected from military fast jet programs/astronauts i.e. pilots whom have experienced high g-forces and can cope with the environment; thereafter when mature suborbital operations are established, this could be relaxed to allow other (airline) pilots to be employed.

4. SAFETY BY DESIGN

Suborbital spaceplanes (or Reusable Launch Vehicles using the US terminology) are designed and operated using a mix of Aviation & Space attributes. So what design standards should be followed? A mixture of both or are forerunners designing on the edge of innovation and designing their way using their own practices, whilst being cognisant of eventual FAA-AST Launch Licensing requirements? This is stated as a question because the FAA-AST are NOT certifying these vehicles.

Space safety standards dictate a Design for Minimum Risk (DMR) philosophy. This includes deriving Fault Tolerance, Safe-Life and Fail Safe criteria (also for aviation). The FAA-AST DMR philosophy within Advisory Circular AC 437.55-1 [9] details the following Safety Precedence Sequence:

- Eliminate hazards (by design or operation)
- Incorporate safety devices
- Provide warning devices
- Develop and implement procedures and training.

Notice that in space the key term is ‘hazard’. Hazards are analysed and then, as part of quantitative analysis (see section 5) a cumulative assessment is made in order to determine whether the Target Level of Safety has been met i.e. top-down analysis. In aviation, although the term hazard is recognised, the focus is on lower level failure conditions associated with failure modes i.e. in order to meet safety objectives such as $1x10^{-9}$ per flying hour for catastrophic events i.e. bottom-up analysis per AC1309 [10].

As part of the FAA-AST requirements for a launch license permit (CFR §437.55) the safety design analysis must consider the following:

(1) Identify and describe hazards, including but not limited to each of those that result from—
(i) Component, subsystem, or system failures or faults;
(ii) Software errors;
(iii) Environmental conditions;
(iv) ***Human errors****;*
(v) Design inadequacies; or
(vi) Procedural deficiencies.

The NTSB report [4] found that the designers (Scaled Composites) had not undertaken human error analysis (as the cause) in relation to decision errors and skill-based errors. The FAA-AST inspectors noted this and for PF04 provided a waiver against §437.55 (for not completing human error or software fault as a causal factor). We all want the nascent industry to succeed and we want innovative designs (we don’t want to ‘stifle’ the industry) BUT we want safety driving success – not waivers for incomplete analysis.

4.1. KEY SAFETY REQUIREMENTS

By understanding space and aviation requirements the authorities and/or designers

could identify key safety requirements that should be achieved in the design. For instance, a space requirement is that any Inadvertent Failure Modes that could result in a catastrophic outcome should have **3 INHIBITS.** This means 3 separate and independent inhibits which could be hardware (physical switches/guards etc.), software (latches) or combination thereof. The IAASS Space Safety Manual [11] is based on the NASA and (European) ECSS standards and rationalised/consolidated into one manual; in relation to 'Functions Resulting in Catastrophic Hazards' the following requirement is stated:
A system function whose inadvertent operation could result in a catastrophic hazard shall be controlled by a minimum of three independent inhibits, whenever the hazard potential exists. One of these inhibits shall preclude operation by a radio frequency (RF) command or the RF link shall be encrypted. In addition, the ground return for the function circuit must be interrupted by one of the independent inhibits. At least two of the three required inhibits shall be monitored.

Unfortunately, the Commercial Space Transportation Advisory Committee (COMSTAC), whom advise the FAA-AST, gave the IAASS Suborbital Safety Guidance Manual the 'Cold-Shoulder' [12]; COMSTAC comprise US space players including XCOR and Virgin Galactic.

Since the SS2 accident and following NTSB findings, Virgin Galactic have undertaken additional systems safety analysis and have implemented modifications to SS2 [13] including:

1. DESIGN: Feather locking pin, controlled by the vehicle flight computer, which prohibits pilots from unlocking the tail section early
    a. Pilots will have a mechanical override if the locking pin fails
2. PROCEDURAL: VG now deciding to keep the feather locked until after the rocket engine has shut down
    a. Pilots will have three- to five minutes to troubleshoot in case of problems before the feather would be needed for re-entry

5. SAFETY TOOLS & TECHNIQUES

There are a number of standard system safety analysis techniques such as Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Failure Modes Effects & Criticality Analysis (FMECA) to name a few [14].
The FAA-AST hazard analysis AC [9] also refers to the System Safety Process AC 431.35-2A [1515], which includes an exemplar Safety Programme Plan (SPP); this AC dictates these standard techniques including the FMECA. This analysis would have identified an inadvertent failure mode, resulting in catastrophic outcome, and hence demanded further mitigation. The FAA-AST provide the following 3-pronged approach (*Figure 3*) and additional detailed methodology (*Figure 4*) within AC 431.35-2A:

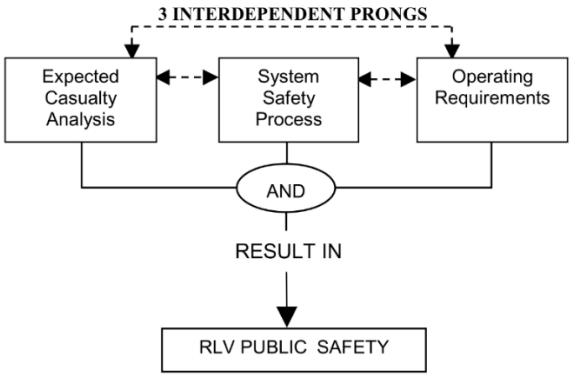

Figure 3: FAA-AST 3-Pronged Safety Approach

The 3-pronged approach includes:

- Expected Casualty Analysis; this relates to analysing the risks to the public in the event of a vehicle break-up, explosion or malfunction turn for instance
- Operating Requirements; this relates to deriving operating procedures and limitations to minimise risk to the public
- System Safety Analysis; this provides detailed guidance for vehicle design organisations in order to derive safety requirements that need to be considered as part of the design (as detailed in the following figure)

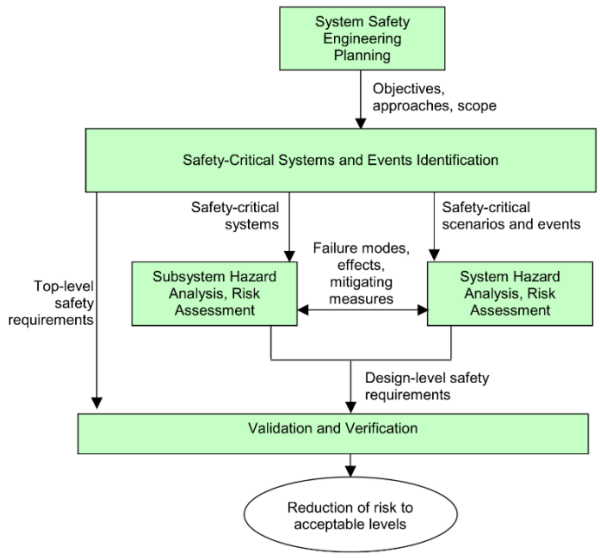

Figure 4: FAA-AST System Safety Engineering Guide

Note in the middle of the figure above, the requirement to undertake a FMECA.

Another safety technique is the Operating and Support Hazard Analysis (OSHA) [16] - here the aim is to analyse the pilot (and maintainer) procedures and the safety engineers then review these to determine whether any hazards are affected by the procedure and also to identify where the human can skip steps or do the steps incorrectly. The FAA OSHA guidelines state that:

This is performed by the Contractor primarily to identify and evaluate hazards associated with the interactions ***between humans and equipment/systems***

Back to the SS2 accident, it was clear that the co-pilot did the procedure step too early as indicated by the red circle below [17] (*Figure 5*):

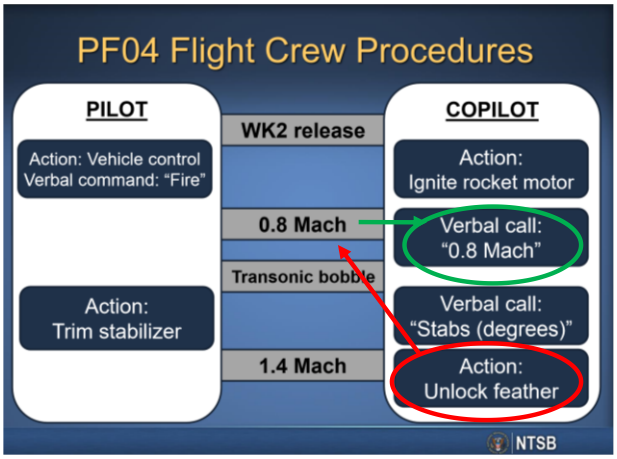

Figure 5: SS2 PF04 Flight Crew Procedures

Note the 'verbal call' at 0.8 Mach that the co-pilot had to make whilst in this busy stressful phase, as well as the trim stabilizer call, followed by the actual unlocking of the feather. The NTSB report notes that the co-pilot had memorised these tasks (from cockpit video footage) rather than read these critical steps from the procedures card (which was on his knee-pad) – which arguably could then have been 'checked' by the pilot.

6. SYSTEM SAFETY & HUMAN FACTORS ENGINEERING DISCIPLINES

This paper has focused on the system safety analysis that is performed (normally) in accordance with standard safety tools and techniques that would address human-machine interactions (both as causes and procedural controls). By undertaking diverse safety analysis, appropriate coverage is provided in order to identify all hazards and provide derived safety requirements (see figure 4) that will then be verified and validated during the development.

Human Factors experts also provide valuable analysis as part of a programme. Here the focus is on human factors integration (or human factors and ergonomics [HFE]) and this includes analysing the cockpit displays for instance i.e. anthropometry, cognitive psychology, display layouts including colours for cautions and warnings etc. and analysing test procedures.

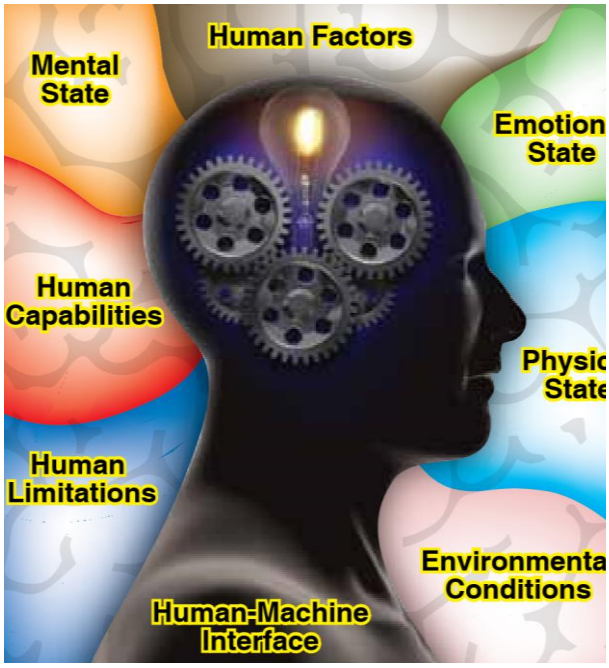

Figure 6: Human Factors that affect performance [18]

In relation to the SS2 PF04 the NTSB Human Performance Presentation noted the following *Stressors* contributing to the accident:

- *Memorization of tasks - Flight test data card not referenced*
- *Time pressure - Complete tasks within 26 seconds - Abort at 1.8 Mach if feather not unlocked*
- *Operational environment - No recent experience with SS2 vibration and load*

The *Stressors* noted above relate to 'human capabilities' in *Figure 6* in that the co-pilot memorized his tasks which needed to be completed by Mach 1.8 and arguably his 'mental state' may have been affected by the 'operational environmental' in the rocket phase of flight (during the transonic bubble) with vibration and noise.

The NTSB report [19] provides further details including details of the cockpit layout and instrumentation i.e. human-machine interface (or ergonomics) aspects. The NTSB found no major contributory factors.

On projects, a problem can exist when the separate disciplines do not work together effectively i.e. design engineers, safety engineers, human factors engineers, software engineers etc. Previous IAASS conferences have had presentations from NASA in their goal for continuous improvement stating that design and safety engineers are now working more closely; and then in a separate presentation stating that designers and HF engineers are working better; well how about all disciplines working together? And how about using safety and human factors specialists with appropriate qualifications, experience and training (from the beginning)?

7. FOCUSING ON THE RIGHT (SAFE) THING

The SS2 accident has highlighted that although initial suborbital pilots *should* originate from flight test schools and still possess similar traits to their earlier (1950s) test pilot brethren, they should be protected by the *right (safe) thing* by design and analysis rather than rely on the *right stuff* due to ineffective design and operating procedures. This paragraph details some aspects of the *right (safe) thing:*

Organisational factors. The co-pilot of SS2 PF04 did not mean to make a critical mistake and arguably contributory factors lay at the organisation level. This relates to the pilot procedures (which should be a safety net to prevent errors) and training; here the procedures were practiced in the simulator, however the simulator cannot realistically replicate the transonic phase with the vibration and noise etc. Professor Nancy Leveson's Systems-Theoretic Accident Model and Processes (STAMP) [20] takes a holistic organisational approach and, *instead of defining safety management in terms of preventing component failure events, it is defined as a continuous control task to impose the constraints (control actions) necessary to limit systems behaviour to safe changes and adaptations*. So here we can learn that particular focus should be spent on analysing the procedures (controls) more effectively to prevent errors – if this means adding design steps to prevent errors, all the better. The simple answer is to always have a check-response (feedback loop, per STAMP) for procedural steps during critical stages of the flight (or indeed design the system such that minimal pilot actions/verbal calls are required).

Human Factors. The suborbital flight profile involves rocket-powered flight at Mach 3, with g-forces, vibration, noise and mix of

atmospheric and space loads. This is extreme interaction of man, the machine and the media (environment) is depicted well within the military-based Operational Risk Management as detailed in the FAA System Safety Handbook [21]:

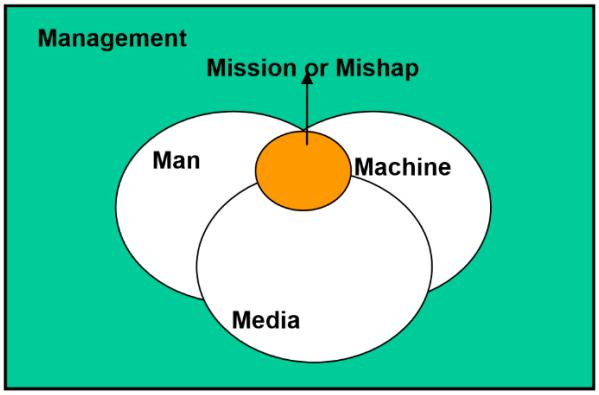

Figure 7: Human Factors 5-M model

The management can have a major influence on whether a suborbital flight results in a successful mission or a mishap (accident). It is the management (organisation) who make the decisions to fly at the Flight Readiness Reviews and who decide on the skillset of the pilots, the safety engineers and the human factors engineers.
A HF specialist should be employed to analyse the HFE aspects, particularly for suborbital flight. This can be based on existing military and civil knowledge base but adapted for the unique suborbital profile.

Safety by Design. It is of no use to have a 'safety officer' employed at some point in the programme to do some 'hazard analysis' to satisfy the FAA-AST requirements. System Safety Engineers should be employed from the concept phase so that they can follow best practice by undertaking detailed and diverse safety analysis. By doing this, derived safety requirements will then be able to influence the design i.e. these will then require design decisions as to acceptance or rejection (with rationale). Such requirements would include levels of fault tolerance, fail-safe and safe life design, and design and development assurance levels. Section 4 further above details the (space) safety precedence sequence using the Design for Minimum Risk approach. The Aerospace Recommended Practices detail the 'typical' development lifecycle from Concept phase to Design Validation & Verification (including testing); this then also is carried through to operations. It is imperative to have a SQEP safety engineer from the start who understands the diverse safety techniques and tools.

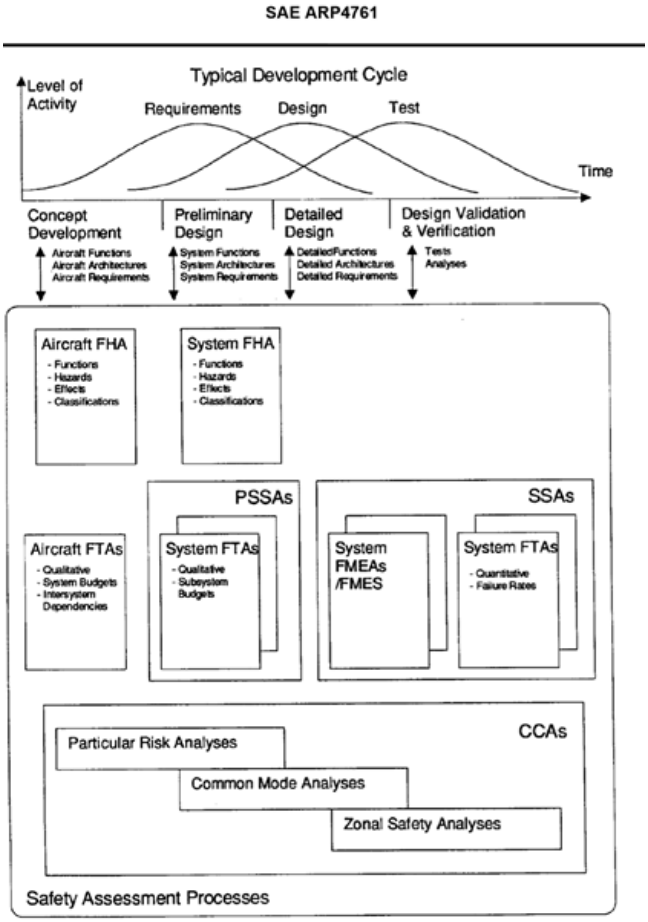

Figure 8: SAE ARP 4761 System Safety Process – detailing typical lifecycle (hence requirement to have safety engineer from the beginning, undertaking diverse and formal safety analysis)

Safety Tools and Techniques (used by SQEP). It is of no use to just have a Fault Tree and hazard log as your safety artefacts. Aviation and space best practice detail diverse safety techniques (and tools) in order to identify hazards (as well as functional failure modes). Indeed, the FAA-AST have reasonable guidance, as detailed in section 5 above. The FAA-AST specifically state that human error analysis (as a cause) should be carried out.
You only know about diverse safety techniques if you have learned about them, have been trained to use them and have used them in appropriate context. Also that your work has been independently checked by experts and/or authorities i.e. you have been

involved in programmes using airworthiness/spaceworthiness standards (meaning that you know about standards and regulations).
So it is vitally important that suborbital operators/designers employ SQEP safety engineers.

8. CONCLUSIONS

This paper reviewed the SS2 accident in order to highlight some of the issues associated with suborbital flights. These flights involve a rocket-power, phase, g-forces and extreme environments and so pilots must be provided with the design and the tools (procedures) to cope with the exacting profile. The pilots must also be suitably fit (medically) and be provided with the 'realistic' training. Why? – so that they **do not** have to rely on the 'right stuff' i.e. flying on the seat of their pants and dealing with problems on their own. By undertaking effective systems safety analysis (per best practice/guidance) then the vehicle will be designed with consideration for safety (from derived safety requirements). The safety (and human factors) analysis will have included human error **as a cause** (as well as considering the human as a control i.e. pilot recovery to a malfunction). The safety analysis would also have covered inadvertent operation/function of a system (by fault or human incorrect selection) and, with a catastrophic outcome, would have derived that 3 Inhibits are required.

So suborbital operators/designers should ensure that the pilots are protected by the *right (safe) thing* by design and analysis rather than rely on the *right stuff.*

9. REFERENCES

[1] Safety Management Manual (SMM), (Doc 9859). International Civil Aviation Organisation, Second Edition, Montreal, 2009

[2] Lautman L and Gallimore P L, (1987), Control of the crew-caused accident: Results of a 12-operator survey, Boeing Airliner, April- June 1-6

[3] Sumwalt R L, (20/9/2012), Obtaining Better Compliance with Standard Operating Procedures (SOPs), NTSB Presentation

[4] NTSB/AAR-15/02 PB2015-10545, Aerospace Accident Report, In-Flight Breakup During Test Flight Scaled Composites SpaceShipTwo, N339SS Near Koehn Dry Lake, California October 31, 2014

[5]https://en.wikipedia.org/wiki/Crew_resource_management

[6] FAA Code of Federal Regulations, Title 14, Chapter III, Subchapter C, Part 460, Human Spaceflight Requirements

[7] IAASS, Suborbital Safety Working Group, Safety Design & Operation of Suborbital Vehicles – Guidance, Issue 2. October 2015

[8] Aerospace Medical Association, Commercial Spaceflight Working Group, Position Paper, Aviation, Space, and Environmental Medicine x Vol. 82, No. 4, April 2011

[9] FAA-AST, Advisory Circular 437.55-1, Hazard Analyses for the Launch or Re-entry of a Reusable Suborbital Rocket Under an Experimental Permit, April 2007

[10] FAA, Advisory Circular 25.1309-1A - System Design and Analysis, 1988

[11] IAASS-ISSB-S-1700-Rev-B, Space Safety Standard, Commercial Human-Rated System, Requirement 201.2.2

[12]http://spacenews.com/40615international-suborbital-safety-proposal-gets-cold-shoulder-in-us by Jeff Foust — May 19, 2014

[13] http://news.discovery.com/space/private-spaceflight/new-virgin-galactic-spaceshiptwo-to-debut-160219.htm

[14] ARP 4761 - Guidelines & Methods for Conducting SSA", Available from: www.sae.org/technical/standards/ARP4761

[15] FAA-AST, Advisory Circular AC 431.35-2A, Reusable Launch and Re-entry Vehicle System Safety Process, July 2005

[16] FAA, FAA-DI-SAFT-105, Operating & Support Hazard Analysis

[17] NTSB, Human and Organisational Issues, Human Performance Presentation, Supporting [4]

[18] FAA, Aviation Maintenance Technician – Handbook, Chapter 14, Figure 14-1

[19] NTSB, Human Factors and Organizational Issues, Human Performance Presentation

[20] Leveson, N: A New Accident Model for Engineering Safer Systems, Massachusetts Institute of Technology paper

[21] FAA System Safety Handbook, Chapter 15: Operational Risk Management December 30, 2000

10. ACRONYMS/ABBREVIATIONS

Abbreviation	Meaning
AAR	Air Accident Report
AC	Advisory Circular
AsMA	Aerospace Medical Association
ATP	Airline Test Pilot
CRM	Crew Resource Management
DMR	Design for Minimum Risk
FAA-AST	Federal Aviation Administration – Office for Commercial Space Transportation
FMECA	Failure Modes Effects & Criticality Analysis
FTA	Fault Tree Analysis
HF	Human Factors
HFE	Human Factors and Ergonomics
NASA	National Aerospace & Space Administration
NTSB	National Transportation Safety Board
OSHA	Operating & Support Hazard Analysis
PRA	Probabilistic Risk Analysis
SMM	Safety Management Manual
SMS	Safety Management System
SOP	Standard Operating Procedure
SPP	Safety Program Plan
SQEP	Suitably Qualified Experienced Personnel
SS2	SpaceShip2
STAMP	Systems-Theoretic Accident Model and Processes
VG	Virgin Galactic